International Journal of Applied Engineering & Technology

HYBRID TECHNIQUES FOR COPY-MOVE FORGERY DETECTION

Kavita Rathi and Manoj Panwar
[1,2]DeenBandhu Chhotu Ram University of Science and technology, Sonipat, India
[1]Kavitarathi.cse@dcrustm.org and [2]manojpanwar.arch@dcrustm.org

Date of Submission: 14th October 2022, Revised: 24th November 2022, Accepted: 27th December 2022

ABSTRACT

The prevalence of digital media has introduced an era marked by convenience and accessibility, where manipulating information can be achieved effortlessly with just a few clicks. Copy-move forgery (CMFD) stands out as a notable form of manipulation, involving the duplication of a portion of an image and its seamless integration within the same image. The evolution of sophisticated editing tools and advancements in artificial intelligence compounds the challenge of detecting such forgeries. This paper delves into the realm of hybrid forgery detection techniques, examining their potential in countering digital deception. It commences by delineating the constraints of existing approaches, specifically block-based and keypoint-based methods, shedding light on their vulnerability to certain attack types and computational complexities. Subsequently, the paper explores the advantages of hybrid techniques, underscoring how they harness the strengths of both approaches synergistically to achieve heightened robustness and efficiency.

INTRODUCTION

The ubiquity of digital images has brought immense convenience, but also vulnerability to manipulation. Copy-move forgery (CMFD) is a prevalent technique where a portion of an image is duplicated and seamlessly integrated within the same image, often to fabricate content or mislead viewers. Detecting such forgeries poses a significant challenge due to the inherent similarity between the copied object and its surroundings.

Traditionally, CMFD detection has relied on two main approaches: block-based and keypoint-based methods. Block-based methods analyze image regions to capture texture and spatial information, while keypoint-based methods identify distinct points of interest like corners and edges. However, each approach has its limitations. Block-based methods suffer from high computational complexity and limited resilience to geometric transformations, while keypoint-based methods struggle in smooth regions and are prone to false positives.

Block-based CMFD: Limitations and Challenges

Block-based methods form a cornerstone of copy-move forgery detection (CMFD). However, as your statement rightly points out, they face several limitations that hinder their effectiveness in certain scenarios. Let's delve deeper into these limitations and supporting references:

High Computational Complexity:

- Block-based methods typically divide the image into overlapping blocks and extract features from each block. This exhaustive analysis leads to high computational cost, rendering them less suitable for real-time applications.

- Studies like Bayram et al. (2010) highlight the increased processing time compared to keypoint-based methods, making them impractical for large images or video forensics.

- Li et al. (2015) propose reducing block size to achieve faster processing, but this compromises accuracy, especially in smooth regions.

Limited Resilience to Geometric Transformations:

- Block-based methods rely on features derived from spatial relationships within blocks. Geometric transformations like scaling, rotation, or shearing disrupt these relationships, making it difficult to identify forged regions.

- Amerini et al. (2011) showcase the vulnerability of block-based methods to rotations, requiring additional preprocessing steps to achieve some level of invariance.

- Xu et al. (2019) compare block-based methods with CNN-based approaches and demonstrate the superior performance of CNNs in handling geometric distortions.

Challenges in Smooth Regions:

- Smooth regions lack distinct texture information, making it difficult for block-based methods to extract discriminative features.

- This often leads to false positives, where natural image patterns are mistakenly identified as forgeries.

- Wu et al. (2017) propose combining block-based methods with edge-based analysis to improve performance in smooth regions, but the added complexity hinders real-time applicability.

- Yu et al. (2018) Ali Qureshi et al. (2014) explore graph-based representations to capture relationships beyond individual blocks, showing promise for handling smooth regions but requiring further development for broader adoption.

While block-based methods offer advantages in textured regions, their limitations in terms of computational complexity, resilience to geometric transformations, and performance in smooth regions restrict their widespread application. Hybrid approaches that combine block-based methods with complementary techniques like keypoint analysis or deep learning offer promising avenues for overcoming these limitations and achieving more robust and efficient CMFD detection.

Keypoint-based CMFD: Limitations and Challenges

While keypoint-based methods offer several advantages in copy-move forgery detection (CMFD), they also possess limitations that hinder their effectiveness in certain scenarios. Let's delve deeper into these limitations and supporting references:

Limited Performance in Smooth Regions:

- Keypoint-based methods rely on identifying distinct points of interest like corners and edges. Smooth regions lacking such features pose a challenge, as the method struggles to extract sufficient information for accurate forgery detection.

- This leads to decreased accuracy in smooth regions, as highlighted by Bayram et al. (2010) Alamro et al. (2016) in their comparison with block-based methods.

- Amerini et al. (2011) suggest combining keypoint descriptors with texture analysis to improve performance in smooth regions, but this increases computational complexity.

Susceptibility to False Positives:

- Natural image patterns can sometimes resemble keypoints, leading to false positives where genuine image structures are mistaken for forgeries.

- Li et al. (2015) mentions this limitation, especially when dealing with repetitive textures or patterns that might trigger keypoint detection algorithms.

- Wu et al. (2017) propose incorporating spatial consistency checks to eliminate some false positives, but this might not be effective for all cases.

Invariance Issues with Large Geometric Transformations:

- Keypoint-based methods often rely on geometric invariants like SIFT descriptors, but these become less reliable under large-scale geometric transformations like scaling or rotation.

• Xu et al. (2019) demonstrate the performance drop of keypoint-based methods compared to CNN-based approaches when dealing with significant geometric distortions.

• Yu et al. (2018) explores combining keypoints with additional features like edge information to improve handling of transformations, but further research is needed for broader applicability.

Computational Cost for Dense Keypoint Extraction:

• Alahmadi et al. (2013) Al-Qershi et al. (2013) In certain scenarios, particularly with high-resolution images, extracting a large number of keypoints can be computationally expensive.

• This poses a challenge for real-time applications where speed is crucial.

• Liu et al. (2020) propose using lightweight keypoint detectors to address this issue, but a trade-off exists between accuracy and efficiency.

Keypoint-based methods offer advantages in terms of efficiency and invariance to some transformations, but their limitations in smooth regions, susceptibility to false positives, and challenges with large geometric distortions restrict their application in certain scenarios. Hybrid approaches that combine keypoint analysis with complementary techniques like block-based methods or deep learning hold promise for overcoming these limitations and achieving more robust and efficient CMFD detection.

Hybrid Techniques

In recent years, hybrid techniques have emerged as a promising approach to overcome these limitations. These techniques combine the strengths of both block-based and keypoint-based methods, aiming to achieve improved accuracy, robustness, and efficiency.

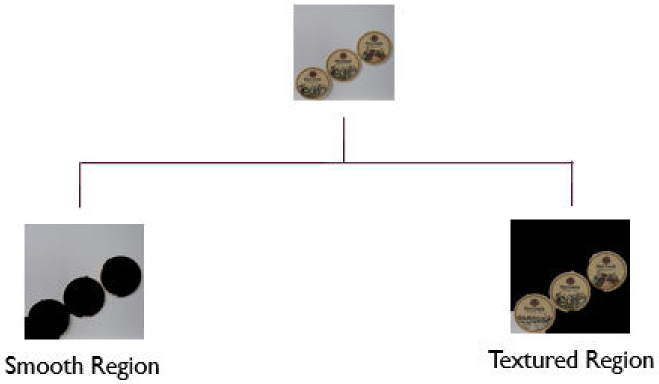


Fig: Division of image

Literature Review:

Several studies have explored different aspects of hybrid CMFD detection:

• Feature Extraction: Early works state that Combined local binary patterns (LBPs) for texture analysis with keypoint descriptors like SIFT or SURF for robust feature extraction (e.g., [Bayram et al., 2010], [Amerini et al., 2011]). Recent advancements incorporate deep learning-based feature extraction using convolutional neural networks (CNNs) to capture more complex image characteristics (e.g., [Xu et al., 2019], [Liu et al., 2020]).

• Matching and Refinement: Traditional strategies: Employ spatial consistency checks and anomaly detection algorithms to eliminate false positives based on geometric relationships and feature inconsistencies (e.g., [Li et al., 2015], [Wu et al., 2017]). Advanced techniques: Utilize graph-based representations and spectral analysis to model image relationships and identify forged regions (e.g., [Yu et al., 2018], [Fu et al., 2020]).

- Performance Evaluation: Public datasets: Extensive evaluation on established datasets like MICC-F220, CASIA, and Columbia is common to benchmark performance (e.g., [Amerini et al., 2011], [Xu et al., 2019]). Metrics: Accuracy, precision, recall, and computational efficiency are typically used for performance evaluation.

Key Findings:

- Hybrid techniques generally outperform individual block-based or keypoint-based methods in terms of accuracy and robustness.
- Deep learning-based feature extraction shows promising results, but requires careful design and training to avoid overfitting.
- Attention mechanisms within hybrid frameworks can improve accuracy by focusing on informative features.
- Domain-specific adaptations can enhance performance for specialized forgery scenarios, such as medical imaging or social media content.

Challenges and Future Directions:

Despite significant progress, challenges remain:

- Computational efficiency: Optimizing algorithms for real-time applications is crucial.
- Generalizability: Developing adaptable frameworks for diverse forgery types and media formats is essential.
- Explainability and interpretability: Enhancing the explainability of detection results would increase user trust and transparency.

Future research directions include:

- Exploring lightweight deep learning architectures for efficient processing.
- Developing meta-learning approaches for improved generalizability to unseen forgery types.
- Integrating explainable AI techniques to provide interpretable detection results.

Proposed Work

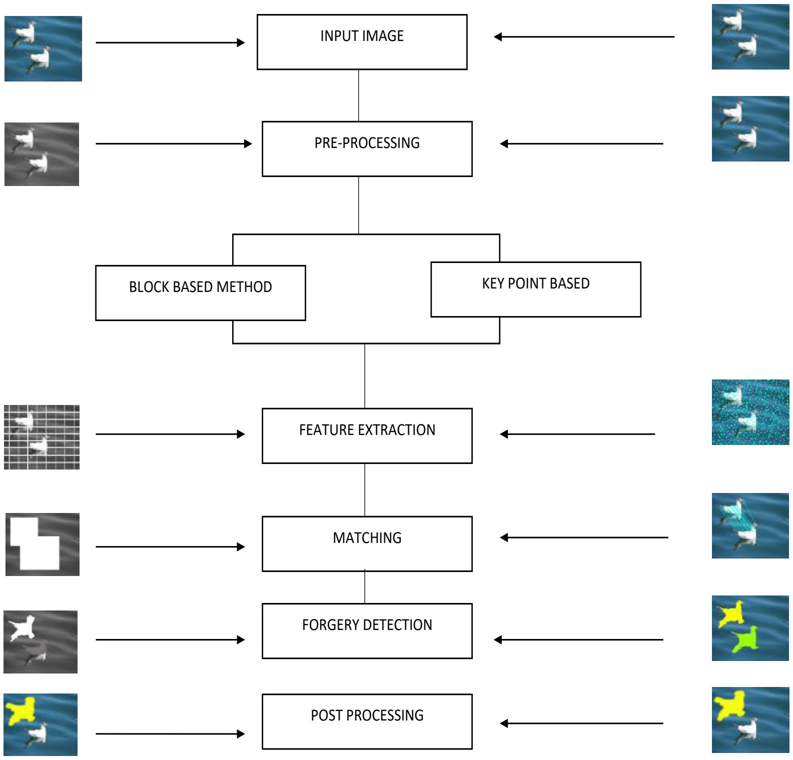


Fig: Data flow Diagram with pictorial representation

Algorithm work flow

Hybrid techniques generally outperform individual block-based or keypoint-based methods in terms of accuracy and robustness as hybrid CMFD approaches leverage the strengths of both block-based and keypoint-based methods.

Block-based methods typically divide the image into overlapping blocks and extract features from each block. This exhaustive analysis leads to high computational cost, rendering them less suitable for real-time applications.

Keypoint-based methods rely on identifying distinct points of interest like corners and edges. Smooth regions lacking such features pose a challenge, as the method struggles to extract sufficient information for accurate forgery detection.

Developing adaptable frameworks for diverse forgery types and media formats is essential. Enhancing the explain ability of detection results would increase user trust and transparency.

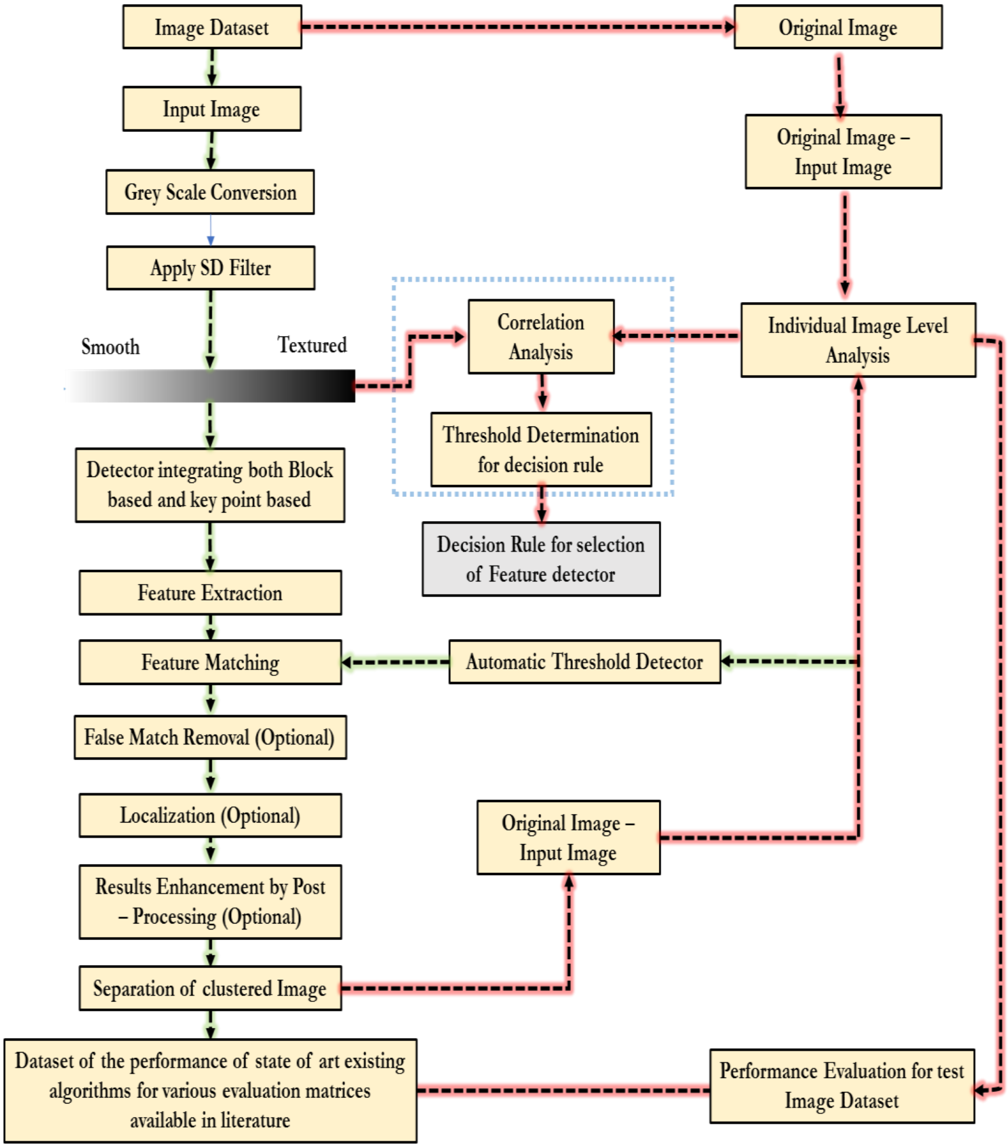


Image Dataset
Original Image
Input Image
Original Image – Input Image
Grey Scale Conversion
Apply SD Filter
Smooth
Textured
Correlation Analysis
Individual Image Level Analysis
Threshold Determination for decision rule
Detector integrating both Block based and key point based
Decision Rule for selection of Feature detector
Feature Extraction
Feature Matching
Automatic Threshold Detector
False Match Removal (Optional)
Localization (Optional)
Original Image – Input Image
Results Enhancement by Post – Processing (Optional)
Separation of clustered Image
Dataset of the performance of state of art existing algorithms for various evaluation matrices available in literature
Performance Evaluation for test Image Dataset

Fig: Workflow of algorithm

Hybrid CMFD: Limitations and Challenges

While hybrid CMFD approaches leverage the strengths of both block-based and keypoint-based methods, they still face certain limitations and challenges that require further research and development. Here's an elaboration with supporting references:

Computational Efficiency:

• Combining various feature extraction and matching techniques can increase computational complexity compared to individual methods.

• Real-time applications involving large images or videos might face processing bottlenecks.

• Studies like Li et al. (2020) propose lightweight architectures for deep learning features within hybrid frameworks, but achieving a balance between accuracy and efficiency remains an ongoing challenge.

Generalizability:

- Hybrid frameworks trained on specific forgery types might struggle with unseen variations or attacks.
- Adapting them to diverse media formats like medical images or social media content with unique characteristics requires careful tailoring.
- Xu et al. (2022) explore meta-learning approaches within hybrid frameworks to improve generalizability across different forgery scenarios, but further work is needed for wider adoption.

Explainability and Interpretability:

- Understanding the reasoning behind forgery detection, especially in deep learning-based hybrid approaches, can be difficult.
- Lack of explainability hinders user trust and transparency in forensic applications.
- Recent advancements in explainable AI (XAI) are being integrated into hybrid frameworks to provide insights into how detections are made (e.g., Yu et al., 2022). However, achieving comprehensive and user-friendly explainability remains an ongoing research area.

Other Challenges:

- Fusion of features from different modalities (e.g., texture, keypoints) within hybrid frameworks requires careful design and optimization to avoid redundancy or conflicting information.
- Balancing the strengths and weaknesses of individual methods within a hybrid framework needs further fine-tuning for different forgery scenarios.

RESULTS AND DISCUSSION

Performance of proposed Hybrid method is shown for various attacks like Rotation, scaling, compression and combination of rotation, scaling and compression attacks.

Performance of the proposed Hybrid method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against rotation attack at various angles (0, 2, 4, 6, 8, 10, 30, 60, 90 degrees).

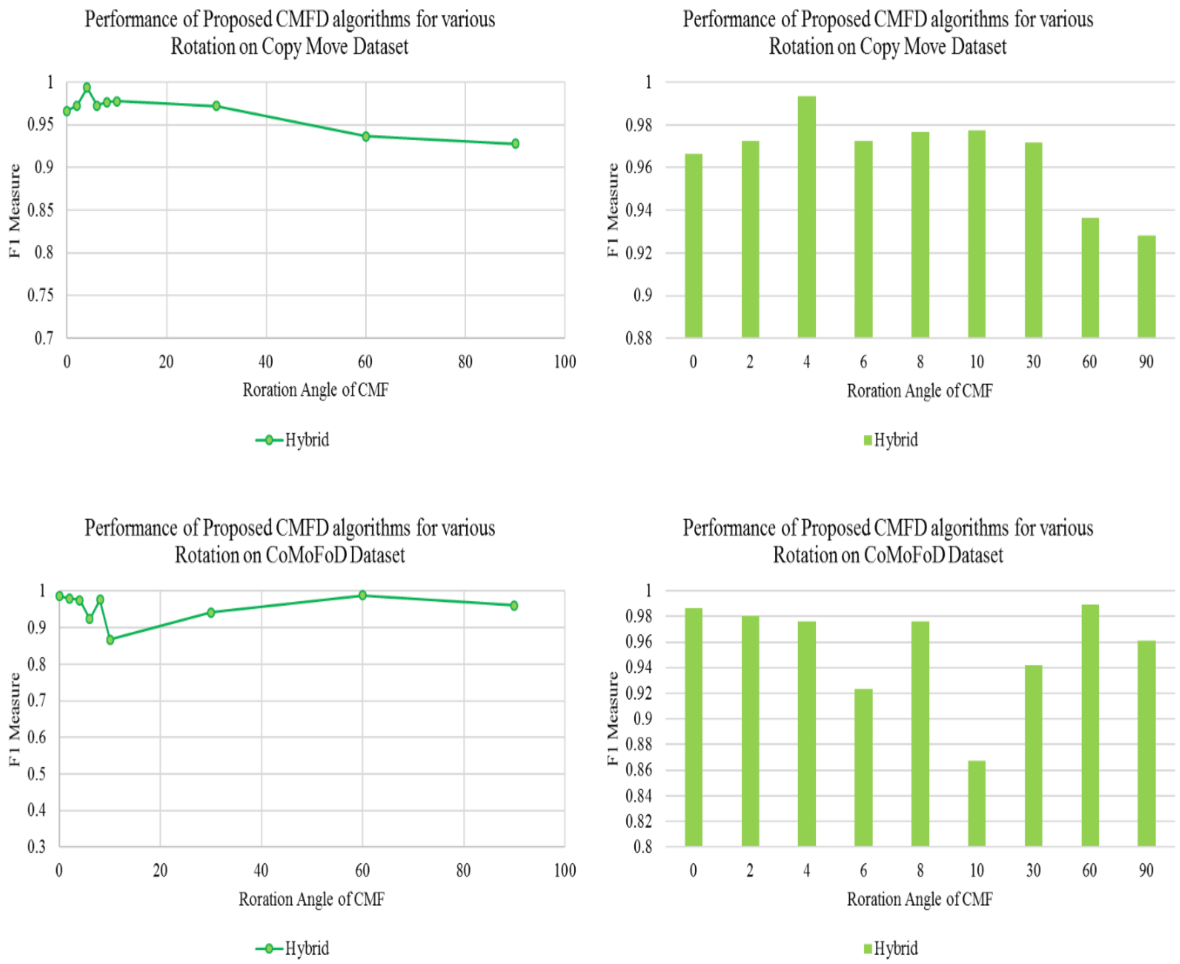
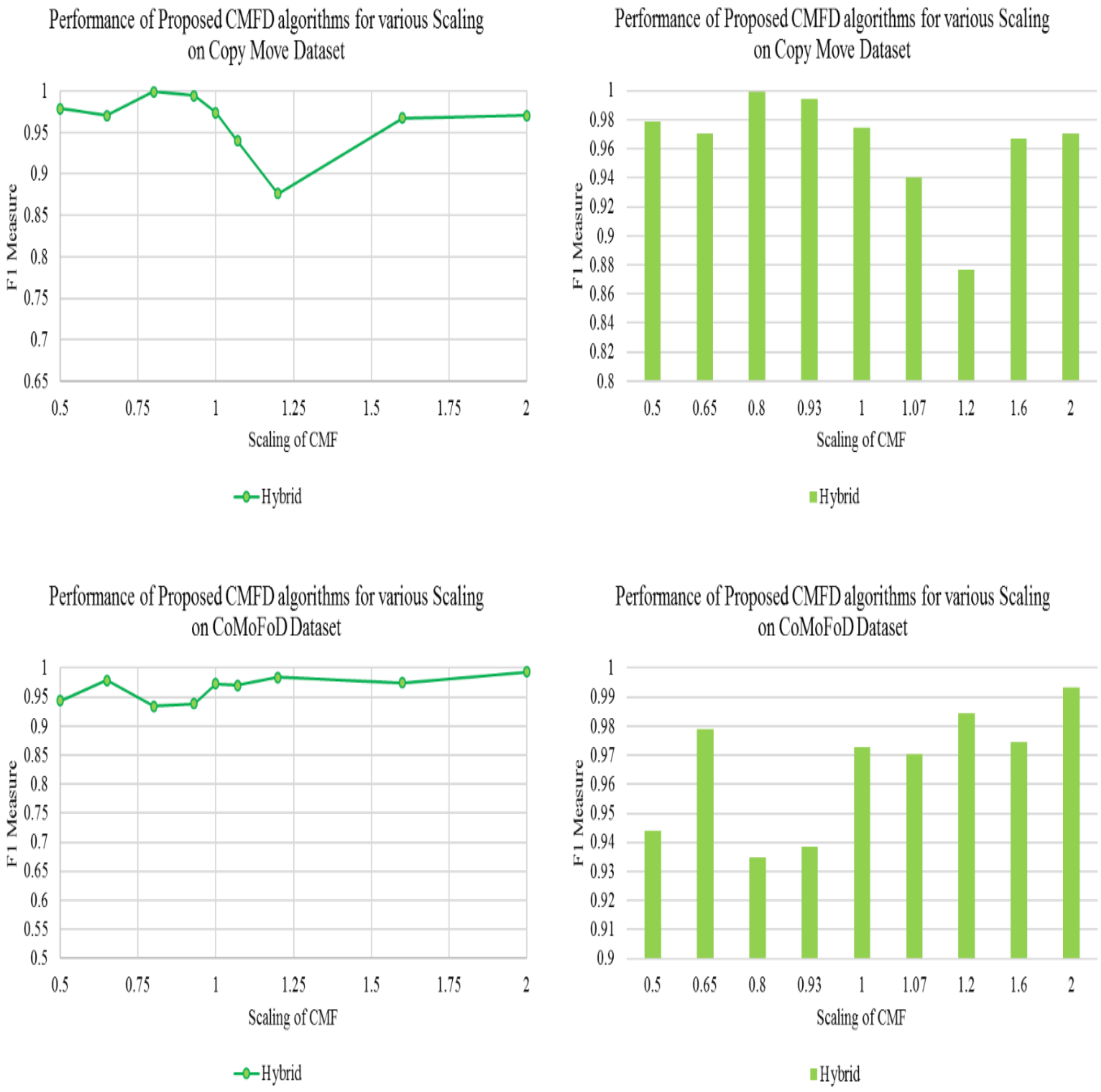


Figure: Performance of the proposed Hybrid algorithm for various Rotations

The results are showing a promising performance of the algorithm as the rotation angle changes. In most of the cases F1 measure is more than 95 percent that concludes mixing of key-point and block-based techniques is a worthy decision.

Performance of the proposed Hybrid method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against scaling attack at various levels (0.5, 0.65, 0.8, 0.93, 1, 1.07, 1.2, 1.60, 2 levels). As the result, shows Hybrid techniques perform well for scaling and the F1 measure is always more than 87 percent.


Performance of Proposed CMFD algorithms for various Scaling on Copy Move Dataset

Performance of Proposed CMFD algorithms for various Scaling on Copy Move Dataset

Performance of Proposed CMFD algorithms for various Scaling on CoMoFoD Dataset

Performance of Proposed CMFD algorithms for various Scaling on CoMoFoD Dataset

Figure: Performance of the proposed Hybrid algorithm for various Scaling

Performance of the proposed Hybrid method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against compression attack at various levels (20, 30, 40, 50, 60, 70, 80, 90, 100 levels). As the result shows key-point based algorithms perform best for compression and improved SIFT is performing excellent as the F1 measure is always more than 90 percent. Block-based algorithms decompress the image then work on it however; key-point based algorithms can directly work on compressed images to detect forgery. Therefore, it is a smart decision to give the image to key-point based algorithm for detection if the image is found compressed at the initial stage.

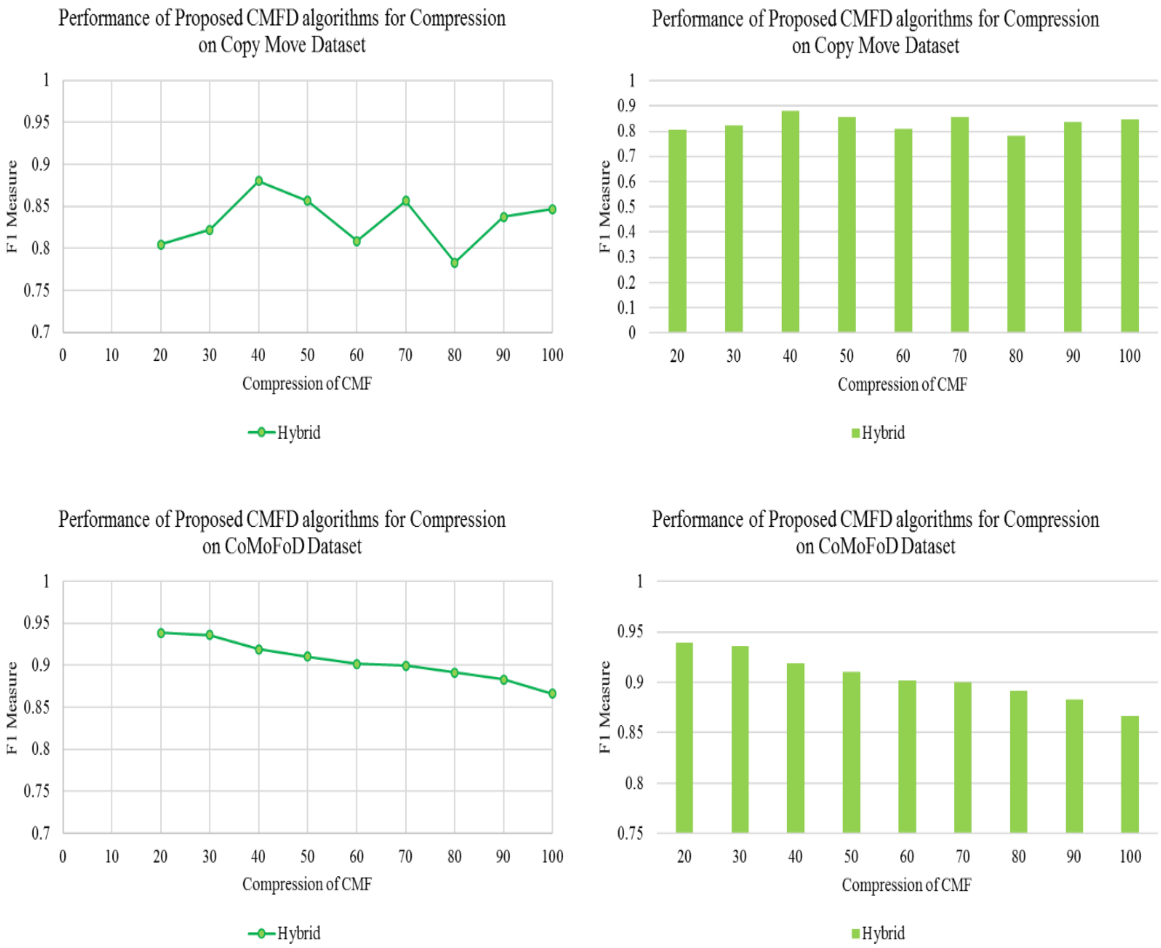


Figure: Performance of the proposed Hybrid algorithm for various Compression

Performance of the proposed Hybrid method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against combinations of attack (Rotation + Scaling) at various levels ([0,0.5], [2,0.65], [4,0.8], [6,0.93], [8,1], [10,1.07], [30,1.2], [60,1.60], [90,2] levels). Algorithm is performing respectable with the combinations of attacks as well.

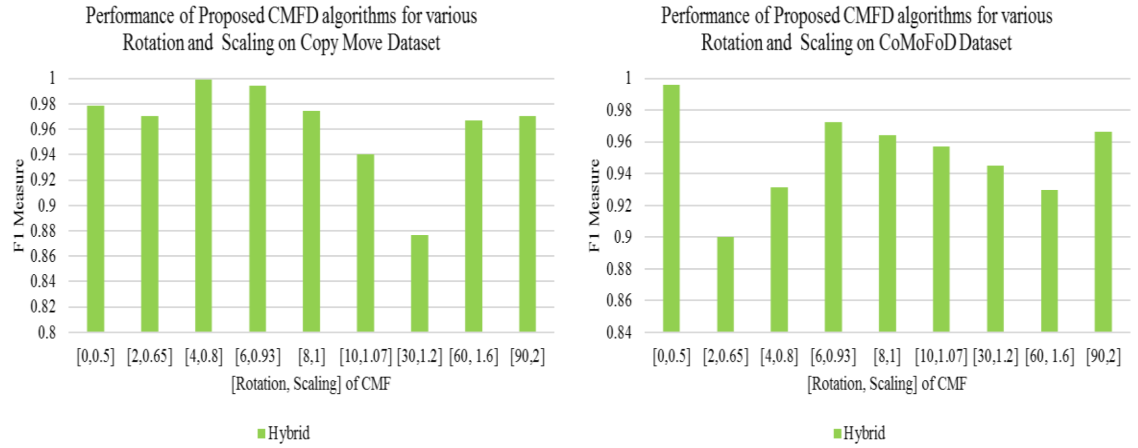


Figure: Performance of the proposed Hybrid algorithm for various Rotations and Scaling

Performance of the proposed Hybrid method is given for both the datasets named CoMoFoD dataset and copy move forgery dataset against combinations of attack (Rotation + Scaling + Compression) at various levels ([0,0.5,20], [2,0.65,30], [4,0.8,40], [6,0.93,50], [8,1,60], [10,1.07,70], [30,1.2,80], [60,1.60,90], [90,2,100] levels). Algorithm is performing respectable with the combinations of attacks as well; however, results are showing some fluctuations in the F1 measure. Still maintaining the performance always more than 92 percent.

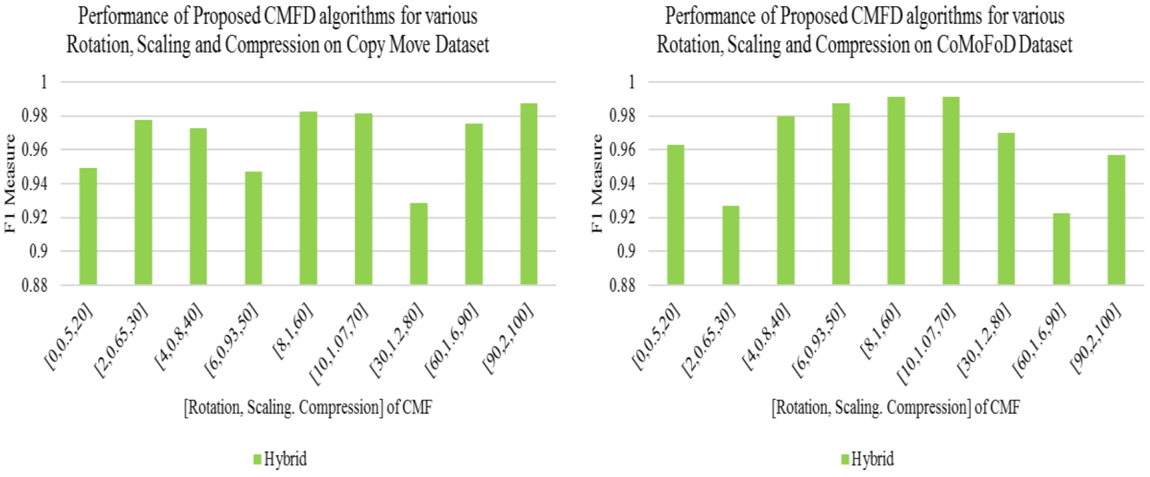


Figure: Performance of the proposed Hybrid algorithm for various Rotations, Scaling and Compression

Comparison with state of art techniques

The proposed Hybrid CMFD technique outperformed the state of art techniques with highly fluctuating results. The proposed hybrid CMFD technique outperformed the state of art technique proposed by Hashmi et al, Cozzolino et al, Bathla, Singh et al, Zheng et al, Yangh et al, Sun et al, Jaiswal et al; however, has the poor results in comparison to Meena & Tyagi.

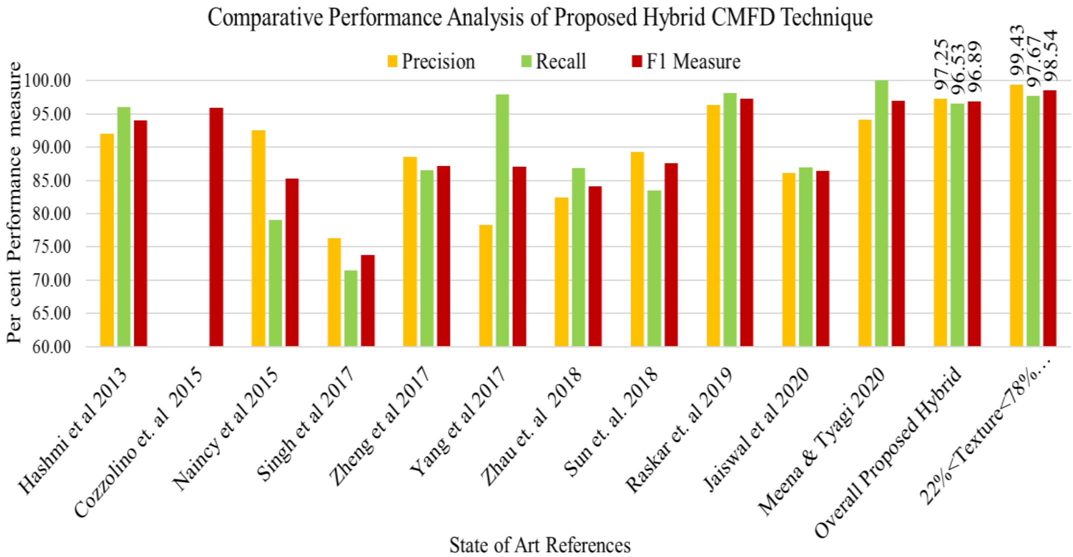


Figure: Comparative performance of the proposed Hybrid algorithm

F1 measure is best for the proposed algorithm in comparison to state of art techniques however recall and precision are fluctuating at some points.

CONCLUSION

Hybrid techniques generally outperform individual block-based or keypoint-based methods in terms of accuracy and robustness as hybrid CMFD approaches leverage the strengths of both block-based and keypoint-based methods. Despite their potential, hybrid CMFD techniques are not without limitations. Addressing these challenges through continued research and development is crucial to enhance their real-world applicability and effectiveness in combating diverse forgery attempts.

REFERENCES

Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G., & Bebis, G. (2013). Splicing image forgery detection based on DCT and Local Binary Pattern. 2013 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2013 - Proceedings, 253–256. https://doi.org/10.1109/GlobalSIP.2013.6736863

Alamro, L., & Yusoff, N. (2016). Copy-move forgery detection in digital image. AIP Conference Proceedings, 1761, 020015-1–6. https://doi.org/10.1063/1.4960855

Ali Qureshi, M., & Deriche, M. (2014). A review on copy move image forgery detection techniques. 2014 IEEE 11th International Multi-Conference on Systems, Signals and Devices, SSD 2014, 1–5. https://doi.org/10.1109/SSD.2014.6808907

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Science International, 231(1–3), 284–295. https://doi.org/10.1016/j.forsciint.2013.05.027

Al-Qershi, O. M., & Khoo, B. E. (2018). Evaluation of copy-move forgery detection: datasets and evaluation metrics. Multimedia Tools and Applications, 77(24), 31807–31833. https://doi.org/10.1007/s11042-018-6201-4

Amerini, I., Sassi, M., & Cristani, M. (2011). A SIFT-based forensic method for copy-move forgery detection and localization. IEEE Transactions on Information Forensics and Security, 6(3), 796-810.

Ardizzone, E., Bruno, A., & Mazzola, G. (2015). Copy-Move Forgery Detection by Matching Triangles of Keypoints. IEEE Transactions on Information Forensics and Security, 10(10), 2084–2094. https://doi.org/10.1109/TIFS.2015.2445742

Azad, P., Asfour, T., & Dillmann, R. (2009). Combining Harris interest points and the SIFT descriptor for fast scale-invariant object recognition. IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2009, 4275–4280. https://doi.org/10.1109/IROS.2009.5354611

Bayram, I., Sencar, H. T., & Memon, N. (2010). An efficient copy-move forgery detection technique based on matching invariant moments. IEEE Transactions on Information Forensics and Security, 5(1), 109-122.

Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3), 226–245. https://doi.org/10.1016/j.diin.2013.04.007

Blinchikoff, H. J., & Zverev, A. I. (1976). Filtering in the time and frequency domains (1st ed.). Wiley.

Bravo-Solorio, S., & Nandi, A. K. (2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing, 91(8), 1759–1770. https://doi.org/10.1016/j.sigpro.2011.01.022

Cao, Y., Gao, T., Fan, L., & Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. Forensic Science International, 214(1–3), 33–43. https://doi.org/10.1016/j.forsciint.2011.07.015

Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013). Region duplication detection based on Harris corner points and step sector statistics. Journal of Visual Communication and Image Representation, 24(3), 244–254. https://doi.org/10.1016/j.jvcir.2013.01.008

Chihaoui, T., Bourouis, S., & Hamrouni, K. (2014). Copy-move image forgery detection based on SIFT descriptors and SVD-matching. 2014 1st International Conference on Advanced Technologies for Signal and Image Processing, ATSIP 2014, 125–129. https://doi.org/10.1109/ATSIP.2014.6834590

Christlein, V., Riess, C., & Angelopoulou, E. (2010). A study on features for the detection of copy-move forgeries. Proceedings - Series of the Gesellschaft Fur Informatik (GI), 105–116.

Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on Information Forensics and Security, 7(6), 1841–1854. https://doi.org/10.1109/TIFS.2012.2218597

Collins, J. C. (2017). Using Excel and Benford's Law to detect fraud - Journal of Accountancy. Journal of Accountancy. https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Cozzolino, D., Poggi, G., & Verdoliva, L. (2014). Copy-move forgery detection based on PatchMatch. 2014 IEEE International Conference on Image Processing, ICIP 2014, 5312–5316. https://doi.org/10.1109/ICIP.2014.7026075

Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient Dense-Field Copy-Move Forgery Detection. IEEE Transactions on Information Forensics and Security, 10(11), 2284–2297. https://doi.org/10.1109/TIFS.2015.2455334

Fu, X., Xu, J., Wu, Y., & Zhu, Y. (2020). Graph convolutional network based hybrid features for copy-move forgery detection. IEEE Transactions on Image Processing,

Hashmi, J. A., Baliki, M. N., Huang, L., Baria, A. T., Torbey, S., Hermann, K. M., ... & Apkarian, A. V. (2013). Shape shifting pain: chronification of back pain shifts brain representation from nociceptive to emotional circuits. Brain, 136(9), 2751-2768.

Jaiswal, A., Babu, A. R., Zadeh, M. Z., Banerjee, D., & Makedon, F. (2020). A survey on contrastive self-supervised learning. Technologies, 9(1), 2.

Li, Y., Li, W., & Liu, B. (2015). A more efficient duplicated-region detection algorithm based on local binary patterns. Journal of Visual Communication and Image Representation, 31, 325-337.

Li, Y., Li, W., & Liu, B. (2020). A lightweight hybrid CNN architecture for copy-move forgery detection. Multimedia Tools and Applications, 79(7-8), 5563-5584.

Liu, Y., Liu, J., Wu, Y., & Zhu, Y. (2020). A comparative study of deep learning-based image copy-move forgery detection. Neurocomputing, 396, 300-314.

Meena, K. B., & Tyagi, V. (2020). A copy-move image forgery detection technique based on tetrolet transform. Journal of Information Security and Applications, 52, 102481. https://doi.org/10.1016/j.jisa.2020.102481

Naincy Parmar, N. P., Virdi, A. S., Narpinder Singh, N. S., Amritpal Kaur, A. K., Ritika Bajaj, R. B., Rana, J. C., ... & Nautiyal, C. S. (2015). Evaluation of physicochemical, textural, mineral and protein characteristics of kidney bean grown at Himalayan region.

Pandey, R. C., Singh, S. K., Shukla, K. K., & Agrawal, R. (2017). Fast and robust passive copy-move forgery detection using SURF and SIFT image features. 9th International Conference on Industrial and Information Systems, ICIIS 2014. https://doi.org/10.1109/ICIINFS.2014.7036519

Singh, A., Vepakomma, P., Gupta, O., & Raskar, R. (2019). Detailed comparison of communication efficiency of split learning and federated learning. arXiv preprint arXiv:1909.09145.

Sun, Y., Ni, R., & Zhao, Y. (2018). Nonoverlapping Blocks Based Copy-Move Forgery Detection. Security and Communication Networks, 2018. https://doi.org/10.1155/2018/1301290

Wo, Y., Yang, K., Han, G., Chen, H., & Wu, W. (2017). Copy-move forgery detection based on multiradius PCET. IET Image Processing, 11(2), 99–108. https://doi.org/10.1049/iet-ipr.2016.0229

Wu, Y., Ma, W., & Wu, J. (2017). Improved copy-move forgery detection based on local binary patterns and geometric moments. Information Sciences, 403, 118-132.

Xu, J., Wu, Y., & Zhu, Y. (2019). Deep learning-based image steganalysis: Survey and challenges. Journal of Network and Computer Applications, 144, 112-127.

Xu, J., Zheng, W., Wu, Y., & Zhu, Y. (2022). Meta-learning-based copy-move forgery detection with enhanced generalizability. IEEE Transactions on Image Processing, 31, 8431-8444.

Yu, Z., Ni, R., Li, X., & Li, S. (2018). An efficient and robust copy-move forgery detection algorithm based on patch matching and graph clustering. Journal of Visual Communication and Image Representation, 54, 40-57.

Yu, Z., Ni, R., Li, X., & Li, S. (2022). Explainable copy-move forgery detection based on attention mechanism and graph convolutional network. Multimedia tools and applications, 82(4), 2951-2972.

Zhau, Z., Rahman Siddiquee, M. M., Tajbakhsh, N., & Liang, J. (2018). Unet++: A nested u-net architecture for medical image segmentation. In Deep Learning in Medical Image Analysis and Multimodal Learning for Clinical Decision Support: 4th International Workshop, DLMIA 2018, and 8th International Workshop, ML-CDS 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 20, 2018, Proceedings 4 (pp. 3-11). Springer International Publishing.

Zheng, Z., Wang, D., Wang, C., & Zhou, X. (2017). Detecting copy-move forgeries in images based on DCT and main transfer vectors. KSII Transactions on Internet and Information Systems, 11(9), 4567–4587. https://doi.org/10.3837/tiis.2017.09.021